DOCID: 4050988

~~SECRET SPOKE~~

UNITED STATES GOVERNMENT

memorandum

DATE: 9 June 1993 Z-043-93

PLS FORWARD TO ADMIRAL STUDEMAN FOR INFO.

REPLY TO ATTN OF: Z

SUBJECT: CIA KRYPTOS Sculpture - Challenge and Resolution ~~(FOUO)~~ - **INFORMATION MEMORANDUM**

TO: DIR

THRU: D/DIR , EXEC/DIR , DDO

Great story!

1. ~~(FOUO)~~ The KRYPTOS sculpture, located at the entrance and in the courtyard of the new CIA headquarters, consists of a series of stone "pages" containing code which begins as International Morse and increases in complexity as the stonework extends into the courtyard. Inserted between these stone "pages" is a flat copper sheet engraved with letters and symbols - the enciphered message - that is the focus of this challenge.

2. (S) ~~(FOUO)~~ In November, a cadre of cryptanalysts assigned to Z Group enthusiastically responded to the challenge. Within one month, three of the four cipher systems used to encrypt the sculpture's plain text had been diagnosed and completely exploited. The cryptographies employed for the encryption of these three parts involved two periodic polyalphabetic substitution ciphers and a keyed columnar transposition cipher. The exploitation of the sculpture's first three parts constitutes a readability of approximately 89%. The final 97 characters continue to elude solution.

3. ~~(FOUO)~~ Attached, for your review, is a brief description of the employed cryptographies and the plain text derived from the three exploited portions of the KRYPTOS sculpture. If your schedule permits, we would be happy to present a 15-minute briefing on the KRYPTOS sculpture solution and introduce you to the cryptanalysts responsible for the success [redacted]

(b)(3)-P.L. 86-36

3 Encls:
1. Copy of Sculpture Picture
2. Copy of Cipher
3. Description of Cryptographies

cc: Z4
Z43

Derived fm: NSA Class. Guide 342-97
29 May 1997
Declassify on: X1, X5

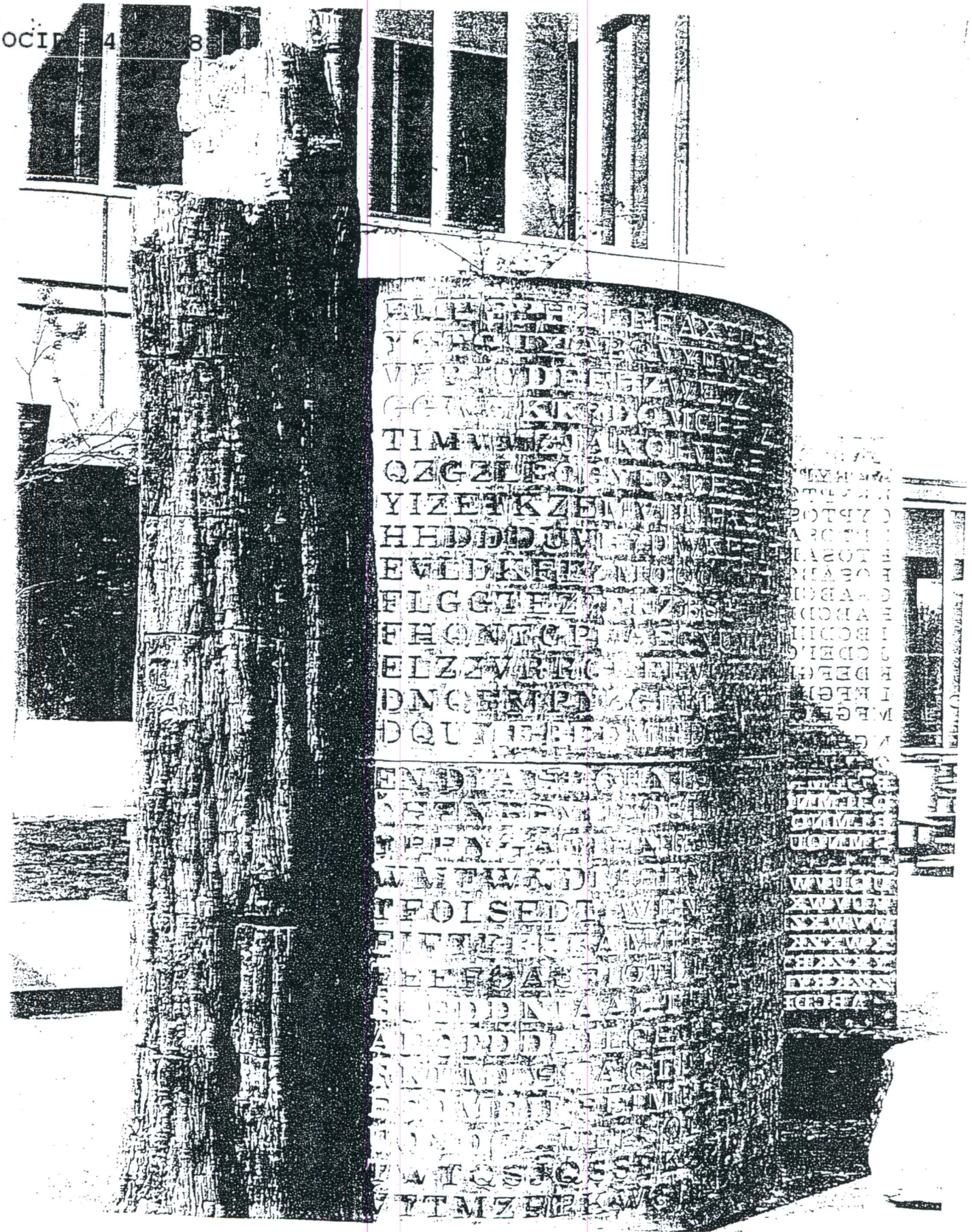
~~SECRET SPOKE~~

~~FOR OFFICIAL USE ONLY~~

OPTIONAL FORM

46695

DOCID: 4 [illegible] 8



(U)

UNCLASSIFIED

DOCID: 4050988

THE KRYPTOS SCULPTURE CIPHER

~~(b)~~

E M U F P H Z L R F A X Y U S D J K Z L D K R N S H G N F I V J
Y Q T Q U X Q B Q V Y U V L L T R E V J Y Q T M K Y R D M F D
V F P J U D E E H Z W E T Z Y V G W H K K Q E T G F Q J N C E
G G W H K K ? D Q M C P F Q Z D Q M M I A G P F X H Q R L G
T I M V M Z J A N Q L V K Q E D A G D V F R P J U N G E U N A
Q Z G Z L E C G Y U X U E E N J T B J L B Q C R T B J D F H J R R
Y I Z E T K Z E M V D U F K S J H K F W H K U W Q L S Z F T I
H H D D D U V H ? D W K B F U F P W N T D F I Y C U Q Z E R E
E V L D K F E Z M O Q Q J L T T U G S Y Q P F E U N L A V I D X
F L G G T E Z ? F K Z B S F D Q V G O G I P U F X H H D R K F
F H Q N T G P U A E C N U V P D J M Q C L Q U M U N E D F Q
E L Z Z V R R G K F F V O E E X B D M V P N F Q X E Z L G R E
D N Q F M P N Z G L F L P M R J Q Y A L M G N U V P D X V K P
D Q U M E B E D M H D A F M J G Z N U P L G E W J L L A E T G
E N D Y A H R O H N L S R H E O C P T E O I B I D Y S H N A I A
C H T N R E Y U L D S L L S L L N O H S N O S M R W X M N E
T P R N G A T I H N R A R P E S L N N E L E B L P I I A C A E
W M T W N D I T E E N R A H C T E N E U D R E T N H A E O E
T F O L S E D T I W E N H A E I O Y T E Y Q H E E N C T A Y C R
E I F T B R S P A M H H E W E N A T A M A T E G Y E E R L B
T E E F O A S F I O T U E T U A E O T O A R M A E E R T N R T I
B S E D D N I A A H T T M S T E W P I E R O A G R I E W F E B
A E C T D D H I L C E I H S I T E G O E A O S D D R Y D L O R I T
R K L M L E H A G T D H A R D P N E O H M G F M F E U H E
E C D M R I P F E I M E H N L S S T T R T V D O H W ? O B K R
U O X O G H U L B S O L I F B B W F L R V Q Q P R N G K S S O
T W T Q S J Q S S E K Z Z W A T J K L U D I A W I N F B N Y P
V T T M Z F P K W G D K Z X T J C D I G K U H U A U E K C A R

UNCLASSIFIED

~~SECRET SPOKE~~

PART 1

~~(SC)~~

Cryptography: Periodic Polyalphabetic Substitution employing 10 alphabets

Plain component: Keyword mixed sequence based on **KRYPTOS**

Cipher component: Keyword mixed sequence based on **KRYPTOS**

Repeating Key: **PALIMPSEST**

Index letter: **K**

P:	**K**	**R**	**Y**	**P**	***T***	**O**	***S***	**A**	***B***	**C**	**D**	***E***	**F**	**G**	**H**	**I**	**J**	**L**	**M**	***N***	**Q**	***U***	**V**	***W***	**X**	**Z**
C1:	P	T	O	S	A	B	C	D	***E***	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y
C2:	A	B	C	D	E	F	G	H	I	J	L	***M***	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S
C3:	L	M	N	Q	***U***	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J
C4:	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	***F***	G	H
C5:	M	N	Q	U	V	W	X	Z	K	R	Y	***P***	T	O	S	A	B	C	D	E	F	G	H	I	J	L
C6:	P	T	O	S	A	B	C	D	E	F	G	***H***	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y
C7:	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	***Z***	K	R	Y	P	T	O
C8:	E	F	G	H	I	J	***L***	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D
C9:	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	***R***	Y	P	T	O
C10:	T	O	S	A	B	C	D	E	***F***	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P

EMUFPHZLRF AXYUSDJKZL DKRNSHGNFI VJYQTQUXQB
BETWEENSUB TLESHADING ANDTHABSCE NCEOFLIGHT

QVYUVLLTRE VJYQTMKYRD MFD
LIESTHENUA NCEOFIQLUS ION

~~(FOUO)~~ Respaced and punctuated, it reads:

"BETWEEN SUBTLE SHADING AND THE ABSENCE OF LIGHT LIES THE NUANCE OF ILLUSION"

~~SECRET SPOKE~~

DOCID: 4050988

~~SECRET SPOKE~~

PART 2

(SCI)

Cryptography: Periodic Polyalphabetic Substitution employing 8 alphabets

Plain component: Keyword mixed sequence based on **KRYPTOS**

Cipher component: Keyword mixed sequence based on **KRYPTOS**

Repeating Key: **ABSCISSA**

Index letter: **K**

```
 P:KRYPTOSABCDEFGHIJLMNQUVWXZ
C1:ABCDEFGHIJLMNQUVWXZKRYPTOS
C2:BCDEFGHIJLMNQUVWXZKRYPTOSA
C3:SABCDEFGHIJLMNQUVWXZKRYPTO
C4:CDEFGHIJLMNQUVWXZKRYPTOSAB
C5:IJLMNQUVWXZKRYPTOSABCDEFGH
C6:SABCDEFGHIJLMNQUVWXZKRYPTO
C7:SABCDEFGHIJLMNQUVWXZKRYPTO
C8:ABCDEFGHIJLMNQUVWXZKRYPTOS
```

VFPJUDEE HZWETZYV GWHKKQET GFQJNCEG GWHKK?DQM
ITWASTOT ALLYINVI SIBLEHOW STHATPOS SIBLE?THE

CPFQZDQM MIAGPFXH QRLGTIMV MZJANQLV KQEDAGDV
YUSEDTHE EARTHSMA GNETICFI ELDXTHEI NFORMATI

FRPJUNGE UNAQZGZL ECGYUXUE ENJTBJLB QCETBJDF
ONWASGAT HEREDAND TRANSMIT TEDUNDER GROUNDTO

HRRYIZET KZEMVDUF KSJHKFWH KUWQLSZF TIHHDDDU
ANUNKNOW NLOCATIO NXDOESLA NGLEYKNO WABOUTTH

VH?DWKBFU FPWNTDKI YCUQZERE EVLDKFEZ MOQQJLTT
IS?THEYSH OULDITSB URIEDOUT THERESOM EWHEREXW

UGSYQPFE UNLAVIDX FLGGTEZ?F KZBSFDQV GOGIPUFX
HOKNOWST HEEXACTL OCATION?O NLYWWTHI SWASHISL

HHDRKFFH QNTGPUAE CNUVPDJM QCLQUMUN EDFQELZZ
ASTMESSA GEXTHIRT YEIGHTDE GREESFIF TYSEVENM

VRRGKFFV OEEXBDMV PNFQXEZL GREDNQFM PNZGLFLP
INUTESSI XPOINTFI VESECOND SNORTHSE VENTYSEV

~~SECRET SPOKE~~

~~SECRET SPOKE~~

MRJQYALM GNUVPDXV KPDQUMZB EDMHDAFM JGZNUPLG
ENDEGREE SEIGHTMI NUTESFOR TYFOURSE CONDSWES

EWJLLAET G
TIDBYROW S

~~(FOUO)~~ Respaced and punctuated, it reads:

"IT WAS TOTALLY INVISIBLE. HOW'S THAT POSSIBLE? THEY USED THE EARTH'S MAGNETIC FIELD. THE INFORMATION WAS GATHERED AND TRANSMITTED UNDERGROUND TO AN UNKNOWN LOCATION. DOES LANGLEY KNOW ABOUT THIS? THEY SHOULD. ITS BURIED OUT THERE SOMEWHERE. WHO KNOWS THE EXACT LOCATION? ONLY W.W. THIS WAS HIS LAST TRANSMISSION. THIRTY-EIGHT DEGREES, FIFTY-SEVEN MINUTES, SIX POINT FIVE SECONDS NORTH. SEVENTY-SEVEN MINUTES, FORTY-FOUR SECONDS WEST. I.D. BY ROWS."

~~(SC)~~ **Note:** W.W. is presumed to be William Webster. The coordinates refer to the location of or a location within the Central Intelligence Agency. The significance of I.D. BY ROWS remains undetermined.

~~SECRET SPOKE~~

~~SECRET SPOKE~~

DOCID: 4050988

PART 3

~~(SC)~~

Cryptography: Keyed Columnar transposition
Matrix size: Incompletely filled 4 X 86
Specific key: **KRYPTOS**, numerically keyed and repeated 13 times
(first 12 columns listed below)
Route: Bottom to top

```
SLOWLYDESPARATLYSLOWLYTHEREMAINSOFPASSAGEDE
ASREMOVEDWITHTREMBLINGHANDSIMADEATINYBREACH
OLEALITTLEIINSERTEDTHECANDLEANDPEEREDINTHEH
FLICKERBUTPRESENTLYDETAILSOFTHEROOMWITHINEM
 1      1      1      9      8      7
 2      1      0
```

```
BRISTHATENCUMBEREDTHELOWERPARTOFTHEDOORWAYW
INTHEUPPERLEFTHANDCORNERANDTHENWIDENINGTHEH
OTAIRESCAPINGFROMTHECHAMBERCAUSEDTHEFLAMETO
ERGEDFROMTHEMISTXCANYOUSEEANYTHINGQ
 6      5      4      3      2      1
```

(U) "SLOWLY DESPARATLY SLOWLY THE REMAINS OF PASSAGE DEBRIS THAT ENCUMBERED THE LOWER PART OF THE DOORWAY WAS REMOVED. WITH TREMBLING HANDS I MADE A TINY BREACH IN THE UPPER LEFT HAND CORNER, AND THEN, WIDENING THE HOLE A LITTLE, I INSERTED THE CANDLE AND PEERED IN. THE HOT AIR ESCAPING FROM THE CHAMBER CAUSED THE FLAME TO FLICKER, BUT PRESENTLY, DETAILS OF THE ROOM WITHIN EMERGED FROM THE MIST X CAN YOU SEE ANYTHING Q"

Note: The above is a paraphrase from The Tomb of Tut-Ankh-Amen written by Mr. Howard Carter.

~~SECRET SPOKE~~

DOCID: 4050989 ~~CONFIDENTIAL~~

SECURITY CLASSIFICATION

NSA STAFF PROCESSING FORM

TO	EXREG CONTROL NUMBER	KCC CONTROL NUMBER	Z CONTROL NUMBER
DDO			Z-054-98

THRU	ACTION	EXREG SUSPENSE
	☐ APPROVAL	
SUBJECT	☐ ACTION	KCC SUSPENSE
CIA KRYPTOS Sculpture -- The Challenge and Resolution (U)	☒ INFORMATION	ELEMENT SUSPENSE

DISTRIBUTION

Z4 [redacted], Z23 [redacted]

(b)(3)-P.L. 86-36

SUMMARY

1. (U) In response to your request we have put together a package chronologically outlining the events in our decryption (89%) of the CIA courtyard KRYPTOS sculpture. Also attached is a copy of the original memorandum to Adm. McConnell with attachments providing the cipher, the cryptography employed, and the respective decrypts.

2. (U) The initial examination of the cipher revealed that it was likely to consist of three cryptographically distinct sections. Basic computer diagnostic tools confirmed this hypothesis. Subsequent analysis and solution, however, did not require any compute power.

3. (C) Parts 1-3 were solved within two days of receiving the informal tasking from Chief, Z. Another day was spent on the final section and a decision was made to stop any further work. Given the suspected cryptography, the last section is too short to solve without diverting a great deal of effort from operational problems.

(b)(3)-P.L. 86-36

COORDINATION/APPROVAL

OFFICE	NAME AND DATE	SECURE PHONE	OFFICE	NAME AND DATE	SECURE PHONE
Z09	[redacted] 7/22	5043s			
			Drafter	[redacted]	4451s

	ORG.	PHONE (Secure)	DATE PREPARED
Z			

[redacted]

FORM A6796 FEB 94
NSN: 7540-FM-001-5465

CLASSIFIED BY: NSA Class Guide 342-97 Dated 29 May 1997
DECLASSIFY ON: X1, X5

~~CONFIDENTIAL~~

Chronological history of NSA personnel and their involvement in the partial decryption of the KRYPTOS sculpture located in the CIA courtyard

- 1988 - The CIA Fine Arts Commission approves James Sanborn's proposal.
- 1990 - The artwork, titled *Kryptos*, is dedicated. A portion of this work of art consists of a classic Vigenere Square and 870 characters of cipher punched through two large copper sheets.
- 1991 - While on a trip to the CIA headquarters, an informal group comprised mainly of Cryptanalysis interns, handwrites the cipher onto sheets of paper , and distributes it to any and all interested cryptanalysts back at NSA.
- 1992 - Official challenge for solution is relayed through DCI at a Gold Bug award ceremony.
- 1992 - Mr. [redacted] is the first person to decrypt a portion of the cipher. The cipher system used is a polyalphabetic substitution using eight alphabets. The decrypted text accounts for the last 373 characters from the first section of 436, but the initial 63 characters resist decryption. Because of this, analysts concede that four distinct sections are likely, with this being the second section. (b)(3)-P.L. 86-36
- 1992 - Mr. [redacted] is the second person to successfully decrypt a portion of the cipher. That portion is the third section involving 337 characters and employing a transposition system using a matrix with dimensions 4 X 86.
- 1992 - As the third successful cryptanalyst, Mr. [redacted] successfully decrypts the initial 63 characters of the cipher, which is the first section. It also uses a polyalphabetic substitution, but with 10 alphabets.
- 1992 - An informal document is produced detailing the solution of the three sections. These three sections comprise the first 773 characters out of 870 total, leaving the last 97 characters unresolved.
- 1993 - A formal letter is sent to Adm. McConnell (DIRNSA) detailing the story, and is returned with a request that it be forwarded to Adm. Studeman at CIA.
- 1998 - There is renewed interest from the CIA, with an eye towards a technical article for an internal publication.

DOCID: 4050989

DONE: EXREG 142-93

UNITED STATES GOVERNMENT

memorandum

DATE: 9 June 1993 Z-043-93

PLS FORWARD TO ADMIRAL STUDEMAN FOR INFO.

REPLY TO ATTN OF: Z

SUBJECT: CIA KRYPTOS Sculpture - Challenge and Resolution ~~(FOUO)~~
INFORMATION MEMORANDUM

TO: DIR

THRU: D/DIR, EXEC/DIR, DDO

Great Story!

1. ~~(FOUO)~~ The KRYPTOS sculpture, located at the entrance and in the courtyard of the new CIA headquarters, consists of a series of stone "pages" containing code which begins as International Morse and increases in complexity as the stonework extends into the courtyard. Inserted between these stone "pages" is a flat copper sheet engraved with letters and symbols - the enciphered message - that is the focus of this challenge.

2. ~~(FOUO)~~ In November, a cadre of cryptanalysts assigned to Z Group enthusiastically responded to the challenge. Within one month, three of the four cipher systems used to encrypt the sculpture's plain text had been diagnosed and completely exploited. The cryptographies employed for the encryption of these three parts involved two periodic polyalphabetic substitution ciphers and a keyed columnar transposition cipher. The exploitation of the sculpture's first three parts constitutes a readability of approximately 89%. The final 97 characters continue to elude solution.

3. ~~(FOUO)~~ Attached, for your review, is a brief description of the employed cryptographies and the plain text derived from the three exploited portions of the KRYPTOS sculpture. If your schedule permits, we would be happy to present a 15-minute briefing on the KRYPTOS sculpture solution and introduce you to the cryptanalysts responsible for the success against this cipher.

[redacted]

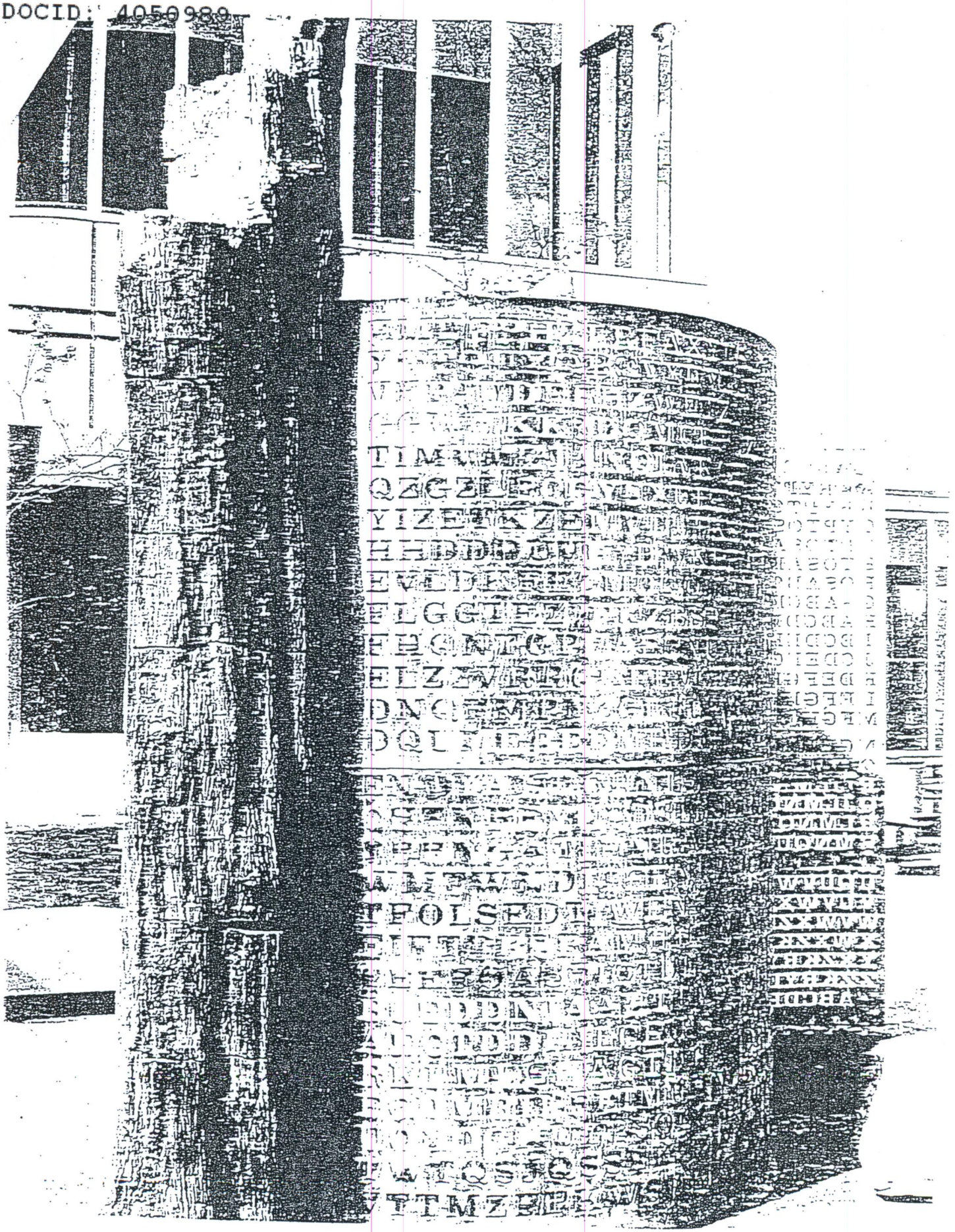
(b)(3)-P.L. 86-36

3 Encls:
1. Copy of Sculpture Picture
2. Copy of Cipher
3. Description of Cryptographies

cc: Z4
Z43

~~FOR OFFICIAL USE ONLY~~

OPTIONAL FORM
46695
6-139



DOCID: 4050989

THE KRYPTOS SCULPTURE CIPHER

E M U F P H Z L R F A X Y U S D J K Z L D K R N S H G N F I V J
Y Q T Q U X Q B Q V Y U V L L T R E V J Y Q T M K Y R D M F D
V F P J U D E E H Z W E T Z Y V G W E K K Q E T G F Q J N C E
G G W H K K ? D Q M C P F Q Z D Q M M I A G P F X H Q R L G
T I M V M Z J A N Q L V K Q E D A G D V F R P J U N G E U N A
Q Z G Z L E C G Y U X U E E N J T B J L B Q C R T B J D F H J R R
Y I Z E T K Z E M V D U F K S J H K F W H K U W Q L S Z F T I
H H D D D U V H ? D W K B F U F P W N T D F I Y C U Q Z E R E
E V L D K F E Z M O Q Q J L T T U G S Y Q P F E U N L A V I D X
F L G G T E Z ? F K Z B S F D Q V G O G I P U F X H H D R K F
F H Q N T G P U A E C N U V P D J M Q C L Q U M U N E D F Q
E L Z Z V R R G K F F V O E E X B D M V P N F Q X E Z L G R E
D N Q F M P N Z G L F L P M R J Q Y A L M G N U V P D X V K P
D Q U M E B E D M H D A F M J G Z N T P L G E W J L L A E T G
E N D Y A H R O H N L S R H E O C P T E O I B I D Y S H N A I A
C H T N R E Y U L D S L L S L L N O E S N O S M R W X M N E
T P R N G A T I H N R A R P E S L N N E L E B L P I I A C A E
W M T W N D I T E E N R A H C T E N E U D R E T N H A E O E
T F O L S E D T I W E N H A E I O Y T E Y Q H E E N C T A Y C R
E I F T B R S P A M H H E W E N A T A M A T E G Y E E R L B
T E E F O A S F I O T U E T U A E O T O A R M A E E R T N R T I
B S E D D N I A A H T T M S T E W P T E R O A G R I E W F E B
A E C T D D H I L C E I H S I T E G O E A O S D D R Y D L O R I T
R K L M L E H A G T D H A R D P N E O H M G F M F E U H E
E C D M R I P F E I M E H N L S S T T R T V D O H W ? O B K R
U O X O G H U L B S O L I F B B W F L R V Q Q P R N G K S S O
T W T Q S J Q S S E K Z Z W A T J K L U D I A W I N F B N Y P
V T T M Z F P K W G D K Z X T J C D I G K U H U A U E K C A R

DOCID: 4050989

PART 1

Cryptography: Periodic Polyalphabetic Substitution employing 10 alphabets
Plain component: Keyword mixed sequence based on **KRYPTOS**
Cipher component: Keyword mixed sequence based on **KRYPTOS**
Repeating Key: **PALIMPSEST**
Index letter: **K**

P:	**K**	**R**	**Y**	**P**	***T***	**O**	***S***	**A**	***B***	**C**	**D**	***E***	**F**	**G**	**H**	**I**	**J**	**L**	**M**	***N***	**Q**	***U***	**V**	***W***	**X**	**Z**
C1:	P	T	O	S	A	B	C	D	***E***	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y
C2:	A	B	C	D	E	F	G	H	I	J	L	***M***	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S
C3:	L	M	N	Q	***U***	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J
C4:	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	***F***	G	H
C5:	M	N	Q	U	V	W	X	Z	K	R	Y	***P***	T	O	S	A	B	C	D	E	F	G	H	I	J	L
C6:	P	T	O	S	A	B	C	D	E	F	G	***H***	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y
C7:	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	***Z***	K	R	Y	P	T	O
C8:	E	F	G	H	I	J	***L***	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D
C9:	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	***R***	Y	P	T	O
C10:	T	O	S	A	B	C	D	E	***F***	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P

EMUFPHZLRF AXYUSDJKZL DKRNSHGNFI VJYQTQUXQB
BETWEENSUB TLESHADING ANDTHABSCE NCEOFLIGHT

QVYUVLLTRE VJYQTMKYRD MFD
LIESTHENUA NCEOFIQLUS ION

~~(TOUO)~~ Respaced and punctuated, it reads:

"BETWEEN SUBTLE SHADING AND THE ABSENCE OF LIGHT LIES THE NUANCE OF ILLUSION"

DOCID: 4050989

PART 2

Cryptography: Periodic Polyalphabetic Substitution employing 8 alphabets
Plain component: Keyword mixed sequence based on **KRYPTOS**
Cipher component: Keyword mixed sequence based on **KRYPTOS**
Repeating Key: **ABSCISSA**
Index letter: **K**

```
 P:KRYPTOSABCDEFGHIJLMNQUVWXZ
C1:ABCDEFGHIJLMNQUVWXZKRYPTOS
C2:BCDEFGHIJLMNQUVWXZKRYPTOSA
C3:SABCDEFGHIJLMNQUVWXZKRYPTO
C4:CDEFGHIJLMNQUVWXZKRYPTOSAB
C5:IJLMNQUVWXZKRYPTOSABCDEFGH
C6:SABCDEFGHIJLMNQUVWXZKRYPTO
C7:SABCDEFGHIJLMNQUVWXZKRYPTO
C8:ABCDEFGHIJLMNQUVWXZKRYPTOS
```

VFPJUDEE HZWETZYV GWHKKQET GFQJNCEG GWHKK?DQM
ITWASTOT ALLYINVI SIBLEHOW STHATPOS SIBLE?THE

CPFQZDQM MIAGPFXH QRLGTIMV MZJANQLV KQEDAGDV
YUSEDTHE EARTHSMA GNETICFI ELDXTHEI NFORMATI

FRPJUNGE UNAQZGZL ECGYUXUE ENJTBJLB QCETBJDF
ONWASGAT HEREDAND TRANSMIT TEDUNDER GROUNDTO

HRRYIZET KZEMVDUF KSJHKFWH KUWQLSZF TIHHDDDU
ANUNKNOW NLOCATIO NXDOESLA NGLEYKNO WABOUTTH

VH?DWKBFU FPWNTDKI YCUQZERE EVLDKFEZ MOQQJLTT
IS?THEYSH OULDITSB URIEDOUT THERESOM EWHEREXW

UGSYQPFE UNLAVIDX FLGGTEZ?F KZBSFDQV GOGIPUFX
HOKNOWST HEEXACTL OCATION?O NLYWWTHI SWASHISL

HHDRKFFH QNTGPUAE CNUVPDJM QCLQUMUN EDFQELZZ
ASTMESSA GEXTHIRT YEIGHTDE GREESFIF TYSEVENM

VRRGKFFV OEEXBDMV PNFQXEZL GREDNQFM PNZGLFLP
INUTESSI XPOINTFI VESECOND SNORTHSE VENTYSEV

DOCID: 4050989

PART 3

Cryptography: Keyed Columnar transposition
Matrix size: Incompletely filled 4 X 86
Specific key: **KRYPTOS**, numerically keyed and repeated 13 times
(first 12 columns listed below)
Route: Bottom to top

```
SLOWLYDESPARATLYSLOWLYTHEREMAINSOFPASSAGEDE
ASREMOVEDWITHTREMBLINGHANDSIMADEATINYBREACH
OLEALITTLEIINSERTEDTHECANDLEANDPEEREDINTHEH
FLICKERBUTPRESENTLYDETAILSOFTHEROOMWITHINEM
 1      1      1      9      8      7
 2      1      0

BRISTHATENCUMBEREDTHELOWERPARTOFTHEDOORWAYW
INTHEUPPERLEFTHANDCORNERANDTHENWIDENINGTHEH
OTAIRESCAPINGFROMTHECHAMBERCAUSEDTHEFLAMETO
ERGEDFROMTHEMISTXCANYOUSEEANYTHINGQ
      6      5      4      3      2      1
```

"SLOWLY DESPARATLY SLOWLY THE REMAINS OF PASSAGE DEBRIS THAT ENCUMBERED THE LOWER PART OF THE DOORWAY WAS REMOVED. WITH TREMBLING HANDS I MADE A TINY BREACH IN THE UPPER LEFT HAND CORNER, AND THEN, WIDENING THE HOLE A LITTLE, I INSERTED THE CANDLE AND PEERED IN. THE HOT AIR ESCAPING FROM THE CHAMBER CAUSED THE FLAME TO FLICKER, BUT PRESENTLY, DETAILS OF THE ROOM WITHIN EMERGED FROM THE MIST X CAN YOU SEE ANYTHING Q".

Note: The above is a paraphrase from The Tomb of Tut-Ankh-Amen written by Mr. Howard Carter.

NSA Artwork turned at CIA
(who wrote the cipher down w/pen & paper)

Dec 91 NSA analysts got together to talk about KRYPTOS sculpture, no further step (intern cipher)

No one got anywhere.

Nov 91/92 CIA did work on the sculpture w/no success

(b)(3)-P.L. 86-36

CIA Challenge ??

[redacted]

Within one week of beginning had the first break

2 wks later 3/4 parts read

Analysts meet w/ [redacted] to explain how/what done [redacted] wanted 100% no 89%

Nothing more was done!

DOCID: 4050994

cipher

#1 polyalphabetic w/ 8 alphabets (2)

#2 transposition (3)

#3 polyalphabetic w/ 10 alphabets (1)

#4 undeciphered

CSSGp Meeting/Activity Notes

(b)(3)-P.L. 86-36

prepared 18 Dec 1991

Yes, the group name is arbitrary (CIA Sculpture Study Group). If you have a better suggestion please let us know. Any other submissions, comments, suggestions, etc. will be welcome and considered.

On 13 December 1991 the first CSSGp analytic meeting was held in conference room 3W083. The discussions were carried on about an hour with all present contributing ideas. Any discussion of "in-house" techniques or applications (being classified) are not mentioned in this text as it is to be unclassified. Other than classified methods to be considered the meeting focused on how to identify the unique "sub-"ciphers of the sculpture in total. (Simplistic worksheets representing these identities are to be included in the distro with this newsletter.)

Also, consideration of the known Morse code parts of the art work are presented on the worksheet contributed by [redacted] (882). Larry's sheet suggests the need for us to have exacting descriptions of all aspects of this work regarding physical placements and relationships in all parts/areas of Sanborn's CIA art presentation. Some of the sculpture is at the Langley HQs front entrance (and this includes most of the Morse code) and other parts are in the central garden (including the punched-copper cipher). The relationship of all the parts of this work are unclear.

Please examine all parts of these mailings to you and then feel free to share your thoughts about them with others on the latest CSSGp analysts listing. To share/distribute any papers you come upon/create before the next meeting mail them yourself or send them to me for copying and I'll distro them asap. I will also mail/phone the notice of any scheduled CSSGp gatherings to those on the analyst listing. Please note that some of the material you get may have distribution caveats/classifications and if they do not consider them as For Official Use Only (FOUO). Do not discuss this effort in public.

[redacted] is attempting to get a video from CIA public info office for the next gathering. This tape will present the morning shows presentation of Sanborn's efforts (apparently some P1 folks have already seen this at CIA). As soon as this is available a meeting will be announced (it may also be a KRYPTOS presentation topic).

On the latest analysts list note the addition of two people, [redacted] (both from A5). They and all those who care to participate are welcome (should we be NOFORN??). The CSSGp is a loose and casual study group where the sharing of ideas to resolve common problems is a primary objective (further definition is

open to discussion also!). The meeting participants will define the direction of effort but each is free for their own exploration (hopefully to be shared later with all). If you wish to remain anonymous/private in your effort let me know and I'll keep that secure. It has been suggested that at some point presentations to KRYPTOS and/or others may be invited.

In attendance at the 13 December gathering were

[redacted] (b)(3)-P.L. 86-36

Again, any new items, distro, news, meeting dates, etc. will be passed on as I get them. Please call me if you want something included.
Happy Hunting! and Happy Holidays!

[redacted]
G411, 963-5315

NOTE: these notes were prepared at NO expense to the US Government

[redacted]
A214 963-5815
OPS2B 2B3036D

(b)(3)-P.L. 86-36

[redacted]
G614 963-4982
HQS 8A198

[redacted]
G963 963-7094
HQS 7A192

[redacted]
G44 963-5401
HQS 2A107

[redacted]
G243 963-4073
HQS 3A045

[redacted]
B82 963-4983
OPS1 3W140

[redacted]
G424 963-6458
OPS1 3A178

[redacted]
G612 963-4716
HQS 8A198

[redacted]
A544 963-1873
OPS2A 2A0336

[redacted]
A544 963-1873
OPS2A 2A0336

[redacted]
A544 963-1873
OPS2A 2A0336

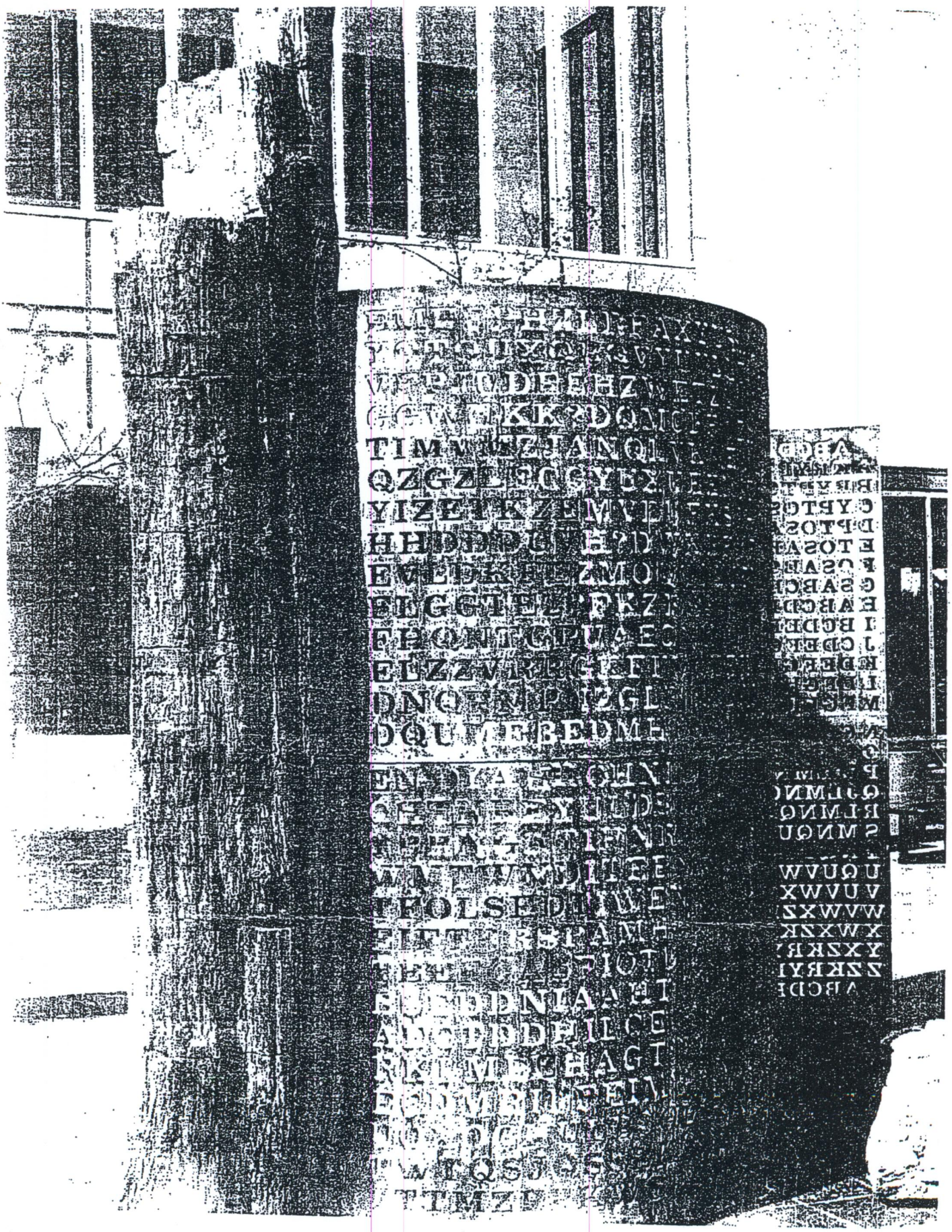
[redacted]
B82 963-4179
OPS1 2S015

[redacted]
B824 963-7132
OPS1 1S025

[redacted]
G411 963-5315
HQS 2A198

EOF

. DOCID: 4050995



. DOCID: 4050995

```
   . . . ..-. -. - .. .-- .. ..-
-> E E E  F  N  T I  W  I  U
<- E E E  L  A  T I  G  I  D

   - .. - -. - . .-. .--. .-. . - .- ..
-> T I  T N  T E  R  P   R  E T A  I
<- T I  T A  T E  R  P   R  E T N  I

   .-. -.. --- --.- ... .. -
->  R  D  O  Q   S  I  T
<-  R  U  O  Y   S  I  T

   . .- --- .. - .. ... ---. .--.
-> E A  O  I  T I  S  O  P
<- E N  O  I  T I  S  O  P

   ... --- ...
->  S  O  S
<-  S  O  S

   . --.- ..-. ..-. -. -.. - .-. .. -... . .
-> E  Q  F  F  N  D  T  R  I  B  E E
<- E  Y  L  L  A  U  T  R  I  V  E E

   . ..-. ...- .. ... .. -... .- .. . . . . .
-> E  F  V  I  S  I  B  A  I  E E E E E
<- E  L  B  I  S  I  V  N  I  E E E E E

   . . --. --- ..- -. .... ... . . .
-> E E  G  O  U  N  H   S  E E E
<- E E  W  O  D  A  H   S  E E E

   . . . . . ... . .-.- .-. --- .-..
-> E E E E E  S  E  ?  R  O  L
<- E E E E E  S  E  C  R  O  F

   . . . ..- .. .-.- -.. ..-.
-> E E E  U  I  ?  D  F
<- E E E  D  I  C  U  L

   . --.- .-. --- -- . --
-> E  Q  R  O M  E M
<- E  Y  R  O M  E M

   -.-- .-.
->  Y  R
<-  Q  R
```

FULL TEXT

FORWARD	BACKWARD
E E E F N T I W I U	D I G I T A L E E E
T I T N T E R P R E T A I	I N T E R P R E T A T I T
R D O Q S I T	T I S Y O U R
E A O I T I S O P	P O S I T I O N E
S O S	S O S
E Q F F N D T R I B E E	E E V I R T U A L L Y E
E F V I S I B A I E E E E E	E E E E E I N V I S I B L E
E E G O U N H S E E E	E E E S H A D O W E E
E E E E E S E ? R O L	F O R C E S E E E E E
E E E U I ? D F	L U C I D E E E
E Q R O M E M	M E M O R Y E
Y R	R Q

DOCID: 4051151

~~CONFIDENTIAL//SI~~

UNITED STATES GOVERNMENT

memorandum

(b)(3)-P.L. 86-36

DATE: 26 March 1992

REPLY TO ATTN OF: [redacted] Z441

SUBJECT: KRYPTOS sculpture

TO: [redacted] Z44

~~(FOUO)~~ In response to a direct challenge from the Central Intelligence Agency, NSA analysts have successfully diagnosed and read a major portion of the KRYPTOS sculpture, located in the courtyard of CIA in Langley, Virginia. As of 1 Dec 92, the cipher has been divided into four sections, with complete analysis and decryption completed on the first 3 parts.

1. ~~(FOUO)~~ Cipher parts 1 and 2 were encrypted using a polyalphabetic substitution system. Part 1 employed 10 alphabets, while part 2 used 8 alphabets. The third section was encrypted using a route transposition on a width of 86.

2. ~~(FOUO)~~ The decrypted text of part 1: "Between subtle shading and the absense of light lies the nuance of iqlusion.[sic]"

3. ~~(FOUO)~~ The decrypted text of part 2: "It was totally invisible. How's that possible? They used the earth's magnetic field. The information was gathered and transmitted underground to an unknown location. Does Langley know about this? They should. It's buried out there somewhere. Who knows the exact location? Only W.W. This was his last message. Thirty-eight degrees, fifty-seven minutes, six point five seconds north. Seventy-seven degrees, eight minutes, forty-four seconds west. I.D. by rows."

4. ~~(FOUO)~~ The decrypted text of part 3: "Slowly, desperatly[sic], slowly, the remains of passage debris that encumbered the lower part of the doorway was removed. With trembling hands I made a tiny breach in the upper left hand corner, and then, widening the hole a little, I inserted the candle and peered in. The hot air escaping from the chamber caused the flame to flicker, but presently, details of the room within emerged from the mist. Can you see anything? Q[sic]"

~~(FOUO)~~ Although ideas abound, a successful break into part 4 has not been made, and analysts continue to work for a solution.

~~CONFIDENTIAL//SI~~

INTRODUCTION

(U) The following paper will take a technical look at the solution to a major portion of the KRYPTOS sculpture located in the courtyard of the Central Intelligence Agency in Langley, Virginia. Before starting on the technical details, let's take a quick look at the history of the sculpture, as well as a few comments from the sculptor.

(U) In June 1988, a Fine Arts Commission project was announced by the CIA to acquire art work for the new CIA Headquarters building. When the selection process had been completed, the Director of Central Intelligence approved the proposal submitted by James Sanborn, a Washington area artist, to create a two-part sculpture at the west entrance to the new Headquarters building, and in the courtyard of the complex. In the fall of 1990 the work was unveiled at a dedication ceremony at the CIA.

(U) According to Mr. Sanborn, "the stonework at the entrance and in the courtyard served two functions. First, it creates a natural framework for the project as a whole and is part of a landscaping scheme designed to recall the natural stone outcropping that existed on the site before the Agency, and that will endure as do mountains. Second, the tilted strata tell a story like pages of a document. Inserted between these stone "pages" is a flat copper sheet through which letters and symbols have been cut. This code, which includes certain ancient ciphers, begins as International Morse and increases in complexity as you move through the piece at the entrance and into the courtyard. Its placement in a geologic context reinforces the text's "hiddenness" as if it were a fossil or an image frozen in time."

(U) This paper's purpose is to concentrate solely on the copper sheets located in the courtyard through which letters and question marks were cut out. It will look at the diagnosis, exploitation and eventual solution of the majority of the cipher contained in the sculpture.

DOCID: 4051151

THE KRYPTOS SCULPTURE

~~(FOUO)~~ One half of the sculpture contains the following Vigenere square, which uses mixed sequences based on the keyword **KRYPTOS**.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
A	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P
B	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T
C	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O
D	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S
E	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A
F	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B
G	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C
H	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D
I	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E
J	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F
K	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G
L	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H
M	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I
N	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L
O	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L
P	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M
Q	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N
R	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q
S	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U
T	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V
U	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W
V	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X
W	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z
X	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K
Y	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R
Z	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

~~(FOUO)~~ The extra letter "**L**" at the end of the 15th line is as it appears in the sculpture. This Vigenere square will turn out to play a key role in reading 2 of the 3 cipher sections exploited by NSA analysts.

~~SECRET~~

U ~~(FOUO)~~ Following is the other half of the main sculpture. Line numbers and underlining have been added for reference purposes only, and are not a part of the sculpture.

```
1   E M U F P H Z L R F A X Y U S D J K Z L D K R N S H G N F I V J
2   Y Q T Q U X Q B Q V Y U V L L T R E V J Y Q T M K Y R D M F D
3   V F P J U D E E H Z W E T Z Y V G W H K K Q E T G F Q J N C E
4   G G W H K K ? D Q M C P F Q Z D Q M M I A G P F X H Q R L G
5   T I M V M Z J A N Q L V K Q E D A G D V F R P J U N G E U N A
6   Q Z G Z L E C G Y U X U E E N J T B J L B Q C R T B J D F H J R R
7   Y I Z E T K Z E M V D U F K S J H K F W H K U W Q L S Z F T I
8   H H D D D U V H ? D W K B F U F P W N T D F I Y C U Q Z E R E
9   E V L D K F E Z M O Q Q J L T T U G S Y Q P F E U N L A V I D X
10  F L G G T E Z ? F K Z B S F D Q V G O G I P U F X H H D R K F
11  F H Q N T G P U A E C N U V P D J M Q C L Q U M U N E D F Q
12  E L Z Z V R R G K F F V O E E X B D M V P N F Q X E Z L G R E
13  D N Q F M P N Z G L F L P M R J Q Y A L M G N U V P D X V K P
14  D Q U M E B E D M H D A F M J G Z N U P L G E W J L L A E T G
15  E N D Y A H R O H N L S R H E O C P T E O I B I D Y S H N A I A
16  C H T N R E Y U L D S L L S L L N O H S N O S M R W X M N E
17  T P R N G A T I H N R A R P E S L N N E L E B L P I I A C A E
18  W M T W N D I T E E N R A H C T E N E U D R E T N H A E O E
19  T F O L S E D T I W E N H A E I O Y T E Y Q H E E N C T A Y C R
20  E I F T B R S P A M H H E W E N A T A M A T E G Y E E R L B
21  T E E F O A S F I O T U E T U A E O T O A R M A E E R T N R T I
22  B S E D D N I A A H T T M S T E W P I E R O A G R I E W F E B
23  A E C T D D H I L C E I H S I T E G O E A O S D D R Y D L O R I T
24  R K L M L E H A G T D H A R D P N E O H M G F M F E U H E
25  E C D M R I P F E I M E H N L S S T T R T V D O H W ? O B K R
26  U O X O G H U L B S O L I F B B W F L R V Q Q P R N G K S S O
27  T W T Q S J Q S S E K Z Z W A T J K L U D I A W I N F B N Y P
28  V T T M Z F P K W G D K Z X T J C D I G K U H U A U E K C A R
```

U ~~(FOUO)~~ An initial look revealed a number of oddities. First was the inclusion of question marks. It was not known if these were being used to signify a transition from one cipher system to another, or if they acted as punctuation for the plaintext. Immediately after the halfway point was the word **END** which may be a coincidence or it might refer to the end of some cryptosystem. This was a distinct possibility because the **Y**, **A**, and **R** that followed **END** were actually raised slightly when compared to the surrounding letters, perhaps signaling the beginning of a different cryptosystem. All of these peculiarities would eventually be explained through the reading of the majority of the cipher.

DIAGNOSIS

~~(S)~~ The initial diagnosis of this cipher revealed the probable use of at least 3 separate cryptographies. The main reason for this assumption was that beginning with line 15, and proceeding through to line 25, numerous analysts noticed that a frequency count of the letters observed would roughly match that of the English language. If lines 15-25 used some particular cryptosystem, then it was likely that another was used for lines 1-14 and yet another one used for lines 26-28. That would yield a probable minimum of 3 distinct cryptosystems in use.

~~(S)~~ A statistical analysis of the first section (lines 1-14) showed a particular roughness on a width of 8. The most common explanation for width roughness is that of a polyalphabetic substitution system. In such a system, a message is encrypted using multiple simple substitutions, employing each substitution in a predetermined order. In this particular case, the width of 8 is a probable indication of 8 cipher alphabets being used.

~~(S)~~ The second section was already partly diagnosed, based solely on analysts "eyeballing" the cipher. Statistical programs confirmed that this section had the characteristics of English plain text, though obviously mixed up in some manner. The most likely explanation for this is a transposition system, perhaps a keyed columnar transposition. In such a system, the plain text is inscribed horizontally into a matrix, normally a rectangle, and then the letters are extracted vertically, according to a predetermined sequence.

~~(C)~~ (S) [redacted] the data also revealed a bias in the third section at an interval of 7. There is no specific cryptography that would give such a result, but a number of them could yield such results under certain circumstances, some of which will be discussed in detail in a later section. After solution of other parts, we discovered that this section was actually the fourth part of the problem. Read on for how this was discovered.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

Secret Source

THE FIRST BREAKTHROUGH

~~(S)~~ Under the hypothesis that the first section employed a polyalphabetic substitution with 8 alphabets, a frequency count was done for each alphabet in the cipher. It was assumed that the alphabets were used in a sequential order, i.e., alphabet #1 was used to encipher characters number 1, 9, 17, 25, etc.; Alphabet #2 was used for characters 2, 10, 18, 26, etc.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
-	-	4	2	2	2	2	2	2	1	1	1	-	8	2	3	2	8	2	-	1	1	3	-	1	4
2	1	-	3	5	4	3	4	-	5	1	4	2	-	-	2	3	3	1	1	3	1	3	-	1	2
3	-	-	3	1	-	7	3	1	3	2	1	1	2	-	-	10	2	1	3	1	3	1	1	4	1
1	3	-	3	1	2	-	-	1	2	7	4	-	4	-	5	2	-	-	4	7	2	-	2	1	3
3	1	1	11	3	7	2	-	2	2	-	2	3	1	-	3	3	-	1	-	3	1	-	1	2	2
1	-	-	4	7	9	1	1	1	1	1	6	2	-	-	-	4	1	-	1	4	-	1	3	1	5
-	2	-	1	6	4	2	3	1	-	-	3	6	1	-	1	1	1	1	5	2	9	-	2	-	3
-	1	2	1	6	3	7	3	-	2	6	1	5	1	1	2	4	-	-	2	3	3	-	-	1	-

~~(S)~~ Using the above frequency counts, it was hoped that one could place the alphabet sequence right on top of each row, though at some offset, and get something that would at least roughly match what you might expect to see. This did not lead to a hoped for solution. Since the accompanying Vigenere Square was based on the keyword **KRYPTOS**, the frequency counts were next sorted based on the same keyword mixed sequence.

K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z
1	8	1	3	-	2	2	-	-	4	2	2	2	2	2	2	1	1	-	8	2	1	1	3	-	4
1	3	1	2	1	-	1	2	1	-	3	5	4	3	4	-	5	4	2	-	3	3	1	3	-	2
2	2	4	-	3	-	1	3	-	-	3	1	-	7	3	1	3	1	1	2	10	1	3	1	1	1
7	-	1	5	4	-	-	1	3	-	3	1	2	-	-	1	2	4	-	4	2	7	2	-	2	3
-	-	2	3	-	-	1	3	1	1	11	3	7	2	-	2	2	2	3	1	3	3	1	-	1	2
1	1	1	-	1	-	1	1	-	-	4	7	9	1	1	1	1	6	2	-	4	4	-	1	3	5
-	1	-	1	5	-	1	-	2	-	1	6	4	2	3	1	-	3	6	1	1	2	9	-	2	3
6	-	1	2	2	1	-	-	1	2	1	6	3	7	3	-	2	1	5	1	4	3	3	-	-	-

~~(S)~~ Using the frequency count this way, it appeared possible to place a keyword mixed alphabet on at least some of these rows. In the third row for example, the following appeared to be a good alignment.

2	2	4	-	3	-	1	3	-	-	3	1	-	7	3	1	3	1	1	2	10	1	3	1	1	1
L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J

DOCID: 4051151

LI ~~(8)~~ In the sixth row the following looked like a good alignment as well.

1 1 1 - 1 - 1 1 - - 4 7 9 1 1 1 1 6 2 - 4 4 - 1 3 5
Q U V W X Z K R Y P T O S A B C D E F G H I J L M N

LI ~~(8)~~ Using some of these assumptions and cribbing in words where needed, a solution was effected. Following are the plain alphabet, the 8 cipher alphabets, and a decryption of the text that was readable. Note two items: **1)** there is a repeating key of **ABSCISSA** under the index letter of **K** in the plain alphabet, and; **2)** the readable text actually begins with the cipher letter **V** at the beginning of the third line of the sculpture.

P:KRYPTOSABCDEFGHIJLMNQUVWXZ
C1: ABCDEFGHIJLMNQUVWXZKRYPTOS
C2: BCDEFGHIJLMNQUVWXZKRYPTOSA
C3: SABCDEFGHIJLMNQUVWXZKRYPTO
C4: CDEFGHIJLMNQUVWXZKRYPTOSAB
C5: IJLMNQUVWXZKRYPTOSABCDEFGH
C6: SABCDEFGHIJLMNQUVWXZKRYPTO
C7: SABCDEFGHIJLMNQUVWXZKRYPTO
C8: ABCDEFGHIJLMNQUVWXZKRYPTOS

VFPJUDEE HZWETZYV GWHKKQET GFQJNCEG GWHKK?DQM
ITWASTOT ALLYINVI SIBLEHOW STHATPOS SIBLE?THE

CPFQZDQM MIAGPFXH QRLGTIMV MZJANQLV KQEDAGDV
YUSEDTHE EARTHSMA GNETICFI ELDXTHEI NFORMATI

FRPJUNGE UNAQZGZL ECGYUXUE ENJTBJLB QCETBJDF
ONWASGAT HEREDAND TRANSMIT TEDUNDER GROUNDTO

HRRYIZET KZEMVDUF KSJHKFWH KUWQLSZF TIHHDDDU
ANUNKNOW NLOCATIO NXDOESLA NGLEYKNO WABOUTTH

VH?DWKBFU FPWNTDKI YCUQZERE EVLDKFEZ MOQQJLTT
IS?THEYSH OULDITSB URIEDOUT THERESOM EWHEREXW

UGSYQPFE UNLAVIDX FLGGTEZ?F KZBSFDQV GOGIPUFX
HOKNOWST HEEXACTL OCATION?O NLYWWTHI SWASHISL

HHDRKFFH QNTGPUAE CNUVPDJM QCLQUMUN EDFQELZZ
ASTMESSA GEXTHIRT YEIGHTDE GREESFIF TYSEVENM

VRRGKFFV OEEXBDMV PNFQXEZL GREDNQFM PNZGLFLP
INUTESSI XPOINTFI VESECOND SNORTHSE VENTYSEV

MRJQYALM GNUVPDXV KPDQUMZB EDMHDAFM JGZNUPLG
ENDEGREE SEIGHTMI NUTESFOR TYFOURSE CONDSWES

EWJLLAET G
TIDBYROW S

U ~~(FOUO)~~ Here is a more readable version, with punctuation added:

"IT WAS TOTALLY INVISIBLE. HOW'S THAT POSSIBLE? THEY USED THE EARTH'S MAGNETIC FIELD. THE INFORMATION WAS GATHERED AND TRANSMITTED UNDERGROUND TO AN UNKNOWN LOCATION. DOES LANGLEY KNOW ABOUT THIS? THEY SHOULD. ITS BURIED OUT THERE SOMEWHERE. WHO KNOWS THE EXACT LOCATION? ONLY W.W. THIS WAS HIS LAST TRANSMISSION. THIRTY-EIGHT DEGREES, FIFTY-SEVEN MINUTES, SIX POINT FIVE SECONDS NORTH. SEVENTY-SEVEN MINUTES, FORTY-FOUR SECONDS WEST. I.D. BY ROWS."

U ~~(FOUO)~~ The reference to **W.W.** is presumed to be William Webster, former director of the CIA. The coordinates given are a location within the CIA grounds, most likely the main complex or the courtyard area. The meaning of **"I.D. BY ROWS"** is not known at this time. The repeating key of **ABSCISSA** is defined by Webster's New World Dictionary as, "the horizontal Cartesian coordinate on a plane, measured from the y-axis along a line parallel with the x-axis to point P".

U ~~(S)~~ After reading this section, it became apparent that the sculpture contained a minimum of 4 parts with one preceding this polyalphabetic section (the first two lines), and two following. More on that a little later.

THE SECOND BREAKTHROUGH

(C//SI) (S) As stated earlier, the section that began at line 15 and most likely finished at line 25 (now referred to as section 3) was a probable transposition system. [redacted] Nonetheless, analysis continued.

(S) The attack that was eventually successful on this portion was one of cribbing by brute force. It was noted that there was a single occurrence of the letter **Q**, and just 5 occurrences of the letter **U**, a likely combination. The 3 or 4 letters surrounding the **Q** were paired with the corresponding letters surrounding each **U**. The results were as follows:

Y N	Y T	Y F	Y T	Y F
T R	T E	T I	T U	T M
E E	E N	E O	E E	E F
Y Y	Y E	Y T	Y T	Y E
Q U	**Q U**	**Q U**	**Q U**	**Q U**
H L	H D	H E	H A	H H
E D	E R	E T	E E	E E
E S	E E	E U	E O	E E
N L	N T	N A	N T	N C

(S) Though many wrong turns were taken, the third pair of columns proved correct and the letter **T** was placed in front of the **HE**, produced the word **THE**. The best combination that matched with the remainder was this:

L Y F
E T I
H E O
A Y T
G **Q U**
T H E
D E T
H E U
A N A

(S) Many of the trigraphs above looked plausible. Using the letter **G** in front of the **QU**, pairs of columns were cribbed to form **INGQU**, with the following alignment yielding the best looking results:

O W L Y F
A M E T I
G T H E O
R W A Y T
I N G Q U
E D T H E
W I D E T
F T H E U
E E A N A

(S) Continuing to use column matching with the remainder of the cipher, a solution was discovered that used an incompletely filled 4 X 86 matrix. That solution follows, but because the matrix is 86 columns wide, the representation has been split into two pieces:

SLOWLYDESPARATLYSLOWLYTHEREMAINSOFPASSAGEDE
ASREMOVEDWITHTREMBLINGHANDSIMADEATINYBREACH
OLEALITTLEIINSERTEDTHECANDLEANDPEEREDINTHEH
FLICKERBUTPRESENTLYDETAILSOFTHEROOMWITHINEM

BRISTHATENCUMBEREDTHELOWERPARTOFTHEDOORWAYW
INTHEUPPERLEFTHANDCORNERANDTHENWIDENINGTHEH
OTAIRESCAPINGFROMTHECHAMBERCAUSEDTHEFLAMETO
ERGEDFROMTHEMISTXCANYOUSEEANYTHINGQ

(S) Further, a very logical key was discovered. The cipher that started this section was from line 15:

E N D Y A H R O H N L S R H E O C P T E O I B I D Y S H N A I

This section can be located in the recovered plaintext, and is inscribed in the matrix from bottom to top, beginning near the end of the message and proceeding towards the front of the message.

SLOWLYDESPARATLYSLOWLYTHEREMAINSOFPASSAGEDE
ASREMOVEDWITHTREMBLINGHANDSIMADEATINYBREACH
OLEALITTLEIINSERTEDTHECANDLEANDPEEREDINTHEH
FLICKERBUTPRESENTLYDETAILSOFTHEROOMWITHINEM
1 1 1 9 8 7
2 1 0

DOCID: 4051151

BRISTHATENCUMBEREDTHELOWERPARTOFTHEDOORWAYW
INTHEUPPERLEFTHANDCORNERANDTHENWIDENINGTHEH
OTAIRESCAPINGFROMTHECHAMBERCAUSEDTHEFLAMETO
ERGEDFROMTHEMISTXCANYOUSEEANYTHINGQ
6 5 4 3 2 1

(S) Proceeding backwards in this manner and labeling each column with a number, it becomes obvious that there is indeed a "method to the madness". What follows is the label for each column written out in order, on a width of 7:

49 12 61 24 73 36 85
48 11 60 23 72 35 84
47 10 59 22 71 34 83
.. ..
.. ..
39 02 51 14 63 26 75
38 01 50 13 62 25 74
37 86

(S) Looked at this way, the patterns within each of the 7 columns are plain, with the possible exception of the "86" at the bottom of the second column. Further, a common procedure in columnar transposition systems is to extract columns of the matrix in an order determined by a specific key, often denoted by a keyword to make the key easy to remember. To generate a numerical key based on a keyword of **KRYPTOS** for example, number the keyword based on alphabetical order:

K	**R**	**Y**	**P**	**T**	**O**	**S**
1	**4**	**7**	**3**	**6**	**2**	**5**

(S) Note how a variation of **KRYPTOS** (spelled backwards and wrapped around the ends) fits the columns of the matrix:

R	**K**	**S**	**O**	**T**	**P**	**Y**
4	**1**	**5**	**2**	**6**	**3**	**7**
49	**12**	**61**	**24**	**73**	**36**	**85**
48	**11**	**60**	**23**	**72**	**35**	**84**
47	**10**	**59**	**22**	**71**	**34**	**83**
..	**..**	**..**	**..**	**..**	**..**	**..**
..	**..**	**..**	**..**	**..**	**..**	**..**
39	**02**	**51**	**14**	**63**	**26**	**75**
38	**01**	**50**	**13**	**62**	**25**	**74**
37	**86**					

(FOUO) Although this may or may not be the way the system was originally set up by Sanborn, it is likely to be very close to the truth. The entire text of section 3 follows, with appropriate punctuation:

"SLOWLY DESPARATLY SLOWLY THE REMAINS OF PASSAGE DEBRIS THAT ENCUMBERED THE LOWER PART OF THE DOORWAY WAS REMOVED. WITH TREMBLING HANDS I MADE A TINY BREACH IN THE UPPER LEFT HAND CORNER, AND THEN, WIDENING THE HOLE A LITTLE, I INSERTED THE CANDLE AND PEERED IN. THE HOT AIR ESCAPING FROM THE CHAMBER CAUSED THE FLAME TO FLICKER, BUT PRESENTLY, DETAILS OF THE ROOM WITHIN EMERGED FROM THE MIST X CAN YOU SEE ANYTHING Q"

(FOUO) In the first line, **DESPERATELY** was misspelled. In the last line, the **X** acts as a period, though other areas of the text should have used periods as well. The **Q** at the end of the text appears to act as a question mark, though the sculpture had a question mark that delineated the end of this section. Earlier, it was noted that in line 15 the **Y**, **A**, and **R** were slightly raised in relation to other surrounding letters. That had no affect on reading this section.

(FOUO) If you have ever read about King Tut, the passage may have sounded familiar to you. It is a paraphrasing from the book **"The Tomb of Tut-ankh-amen"** written by Howard Carter.

THE THIRD BREAKTHROUGH

(S) The last portion read was the first 2 lines of the cipher, section 1. A statistical analysis revealed that this section had width properties that were significant, similar to the first breakthrough, but this time on a width of 5, again implying a polyalphabetic system. Assuming another polyalphabetic system using 5 alphabets, the frequency count follows:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	-	-	2	1	-	-	2	-	-	-	1	2	-	-	-	2	-	-	-	-	2	-	-	-	-
-	-	-	-	-	1	1	-	-	3	2	1	1	-	-	-	-	-	-	-	1	1	-	1	-	1
-	-	-	1	-	-	-	-	-	-	1	1	-	1	-	-	-	1	-	1	1	-	-	1	5	-
-	-	-	-	-	2	-	-	-	-	-	-	-	1	-	-	3	3	-	-	2	-	-	-	-	1
-	1	-	1	1	1	-	-	1	-	-	1	-	-	-	1	-	-	2	2	-	1	-	-	-	-

(S) As before, it was hoped that you could place another alphabet on top of these frequency counts, hopefully resulting in something that would match up nicely. Since the keyword-mixed alphabet based on **KRYPTOS** was used before, we expected that it might be a good choice here. Therefore, a frequency count based on that assumption is given below:

K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z
-	-	-	-	-	-	-	1	-	-	2	1	-	-	2	-	-	1	2	-	2	-	2	-	-	-
2	-	-	-	-	-	-	-	-	-	-	-	1	1	-	-	3	1	1	-	-	1	1	-	1	1
1	1	5	-	1	-	-	-	-	-	1	-	-	-	-	-	-	1	-	1	-	1	-	-	1	-
-	3	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-	-	1	3	2	-	-	-	1
-	-	-	1	2	-	2	-	1	-	1	1	1	-	-	1	-	1	-	-	-	-	1	-	-	-

(S) The small number of characters made solution difficult in either case, but as before, analysis continued. Beginning with a likely starting point, the third alphabet with cipher value **Y** appearing 5 times was assumed to be a plain value **E**. Due to a higher occurrence of the more common letters, the output appeared to be better using the **KRYPTOS** alphabet, which results in the following:

EMUFP HZLRF AXYUS DJKZL DKRNS HGNFI VJYQT QUXQB
..T.. ..S.. ..E.. ..I.. ..D.. ..B.. ..E.. ..G..

QVYUV LLTRE VJYQT MKYRD MFD
..E.. ..N.. ..E.. ..L.. ..N

(S) Through trial and error, another **KRYPTOS** alphabet was placed against the frequencies in the first alphabet, which

yielded the following reasonable text patterns:

EMUFP HZLRF AXYUS DJKZL DKRNS HGNFI VJYQT QUXQB
B.T.. E.K.. T.E.. A.C.. A.D.. E.Y.. N.E.. L.A..

QVYUV LLTRE VJYQT MKYRD MFD
L.E.. H.G.. N.E.. I.E.. I.N

With those recoveries in place, further progress was soon made. It was noted that if the last 3 letters of plain were **ION**, then cipher VJYQT (which occurs twice) would become plain **NCE..**

EMUFP HZLRF AXYUS DJKZL DKRNS HGNFI VJYQT QUXQB
BET.. EMK.. TLE.. ACC.. AND.. ESY.. NCE.. LHA..

QVYUV LLTRE VJYQT MKYRD MFD
LIE.. HDG.. NCE.. INE.. ION

While portions of the text seemed to have good recoveries, such as **AND**, **NCE**, **LIE**, and **ION**, other portions appeared less encouraging, like **EMK**, and **HDG**. Further scrutiny revealed that the "good" recoveries occurred in *every other group* of 5 letters. Using 10 alphabets instead of 5 would eliminate the "bad" recoveries. Looking back at the width statistics, width 10 had also scored high, and the width of 5 was probably a reflection of that.

EMUFPHZLRF AXYUSDJKZL DKRNSHGNFI VJYQTQUXQB
BET..... TLE..... AND..... NCE.....

QVYUVLLTRE VJYQTMKYRD MFD
LIE..... NCE..... ION

Evaluating this new approach, it seemed that the end of the text should be **TION** or **SION**, and that the 2 occurrences of **NCE** would be preceded by a vowel. The following alignment of the tenth alphabet provided that:

EMUFPHZLRF AXYUSDJKZL DKRNSHGNFI VJYQTQUXQB
BET.....B TLE.....G AND.....E NCE.....T

QVYUVLLTRE VJYQTMKYRD MFD
LIE.....A NCE.....S ION

~~(S)~~ Notice that the 2 occurrences of **NCE** are preceded by **E** and **A**, exactly as expected. Further cribbing ensued, which eventually yielded the following set of alphabets and the following decryption:

P:	**K**	**R**	**Y**	**P**	**T**	**O**	**S**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**L**	**M**	**N**	**Q**	**U**	**V**	**W**	**X**	**Z**
C1:	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y
C2:	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S
C3:	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J
C4:	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H
C5:	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L
C6:	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y
C7:	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O
C8:	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D
C9:	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O
C10:	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P

EMUFP HZLRF AXYUS DJKZL DKRNS HGNFI VJYQT QUXQB
BETWE ENSUB TLESH ADING ANDTH ABSCE NCEOF LIGHT

QVYUV LLTRE VJYQT MKYRD MFD
LIEST HENUA NCEOF IQLUS ION

(FOUO) Respaced and punctuated, it reads:

"BETWEEN SUBTLE SHADING AND THE ABSENCE OF LIGHT LIES THE NUANCE OF ILLUSION"

~~(FOUO)~~ In the original decrypt, the word **ILLUSION** was misspelled as **IQLUSION**. The source of this quote is currently unknown. The repeating key of **PALIMPSEST**, below the index letter **K**, has a very interesting definition when viewed in conjunction with the sculpture. It is defined by Webster's New World Dictionary as, "a parchment, tablet, etc., that has been written upon or inscribed two or three times, the previous text or texts having been imperfectly erased and remaining, therefore, still partly visible". Another definition from Webster's Third New International Dictionary is "a memorial brass having earlier engraving on the side opposite to that which is exposed".

THE FOURTH BREAKTHROUGH??

~~(S)~~ Unfortunately, a fourth breakthrough has not yet occurred. There are only 97 characters remaining in section 4, but the first section contained just 63 characters and was exploited, meaning a solution is certainly possible, depending on the cryptosystem. A statistical analysis of this portion showed some roughness on interval 7. This could be a characteristic of plaintext auto-key, *if* the alphabet used has a high frequency letter assigned the value of 0. Another hypothesis is that this last section employs both of the systems already used. First the message is encrypted using some set of alphabets, as was done in the first and third breakthroughs, and then the cipher is put through a transposition, such as that used in the second breakthrough. If the original text had a repeat at a distance of 7 apart (or perhaps 14 or even 21 apart), then after transposing the text, the repeat would now show up in the interval statistic rather than the width statistic.

~~(S)~~ There is no solution at the current time, although some attempts have been made using plaintext auto-key and other attempts using transposed substitution as the enciphering mechanism.

RECAP

U ~~(FOUO)~~ The first section that reads are the first 2 full lines of cipher, a total of 63 characters. The cryptography is a periodic polyalphabetic substitution system employing 10 alphabets. The plain and cipher components are both a keyword mixed sequence based on **KRYPTOS**, using a repeating key of **PALIMPSEST** below the index letter **K**. The plaintext reads:

"BETWEEN SUBTLE SHADING AND THE ABSENCE OF LIGHT LIES THE NUANCE OF ILLUSION"

U ~~(FOUO)~~ The second part reads using the cipher from lines 3-14, a total of 370 characters. The cryptography is another periodic polyalphabetic substitution, employing 8 alphabets. The plain and cipher components are both a keyword mixed sequence based on **KRYPTOS**, using a repeating key of **ABSCISSA** below the index letter **K**. The plaintext reads:

"IT WAS TOTALLY INVISIBLE. HOW'S THAT POSSIBLE? THEY USED THE EARTH'S MAGNETIC FIELD. THE INFORMATION WAS GATHERED AND TRANSMITTED UNDERGROUND TO AN UNKNOWN LOCATION. DOES LANGLEY KNOW ABOUT THIS? THEY SHOULD. ITS BURIED OUT THERE SOMEWHERE. WHO KNOWS THE EXACT LOCATION? ONLY W.W. THIS WAS HIS LAST TRANSMISSION. THIRTY-EIGHT DEGREES, FIFTY-SEVEN MINUTES, SIX POINT FIVE SECONDS NORTH. SEVENTY-SEVEN MINUTES, FORTY-FOUR SECONDS WEST. I.D. BY ROWS."

U ~~(FOUO)~~ The third section uses the cipher contained in lines 14 through the question mark in line 25. The cryptography is a keyed columnar transposition. The matrix is an incompletely filled 4 X 86, using a key of **KRYPTOS** that has been numerically keyed and repeated 13 times. The plaintext reads:

"SLOWLY DESPARATELY SLOWLY THE REMAINS OF PASSAGE DEBRIS THAT ENCUMBERED THE LOWER PART OF THE DOORWAY WAS REMOVED. WITH TREMBLING HANDS I MADE A TINY BREACH IN THE UPPER LEFT HAND CORNER, AND THEN, WIDENING THE HOLE A LITTLE, I INSERTED THE CANDLE AND PEERED IN. THE HOT AIR ESCAPING FROM THE CHAMBER CAUSED THE FLAME TO FLICKER, BUT PRESENTLY, DETAILS OF THE ROOM WITHIN EMERGED FROM THE MIST. CAN YOU SEE ANYTHING?"

U ~~(FOUO)~~ The fourth part has not been read, but most likely uses the last 4 characters of line 25, as well as the cipher in lines 26-28, for a total of 97 characters. It is highly probable

that **KRYPTOS** plays an integral part in the solution, as it did in the 3 parts that have been exploited.